UNITED STATES PATENT AND TRADEMARK OFFICE

mN

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/633,658	08/05/2003	Hideo Sato	241199US6	5298

22850   7590   07/30/2007

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER
TOLENTINO, RODERICK

ART UNIT	PAPER NUMBER
2134	

NOTIFICATION DATE	DELIVERY MODE
07/30/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	10/633,658	SATO, HIDEO
	Examiner	Art Unit	
	Roderick Tolentino	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>21 May 2007</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>*1-20*</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>*1-20*</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>05 August 2003</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1 – 20 are pending.

Response to Arguments

2.   Applicant's arguments with respect to claim 1 have been considered but are moot

in view of the new ground(s) of rejection, as necessitated by amendment made by

applicant on 05/21/2007.

3.   With regards to 35 U.S.C. 101 rejections and 35 U.S.C. 112 1st paragraph

rejections, arguments and amendments have been deemed persuasive and the

rejections have been withdrawn.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically teachd or described as set forth
> in section 102 of this title, if the differences between the subject matter sought to be patented and the
> prior art are such that the subject matter as a whole would have been obvious at the time the invention
> was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

5.   Claims 1, 2, 5, 6, 9, 11, 13, 14, 17 and 18 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Garib U.S. Patent No. (6,728,378) in view of Dyer et al. U.S

Patent No. (6,625,592).

6.   As per claims 1 and 13, Garib teaches a public key encryption processing means

for performing an encryption operation using a public key encryption technique to

generate encrypted data (Garib, Col. 15 Lines 14 – 17, encrypting an unencrypted

message using public key), hash value generation means for generating a hash value

which is used by the public key encryption processing means and storage means for

storing the hash value, (Garib, Col. 5 Lines 66 – 67 and Col. 6 Lines 1 – 6, generates a

hash and stores the hash), but fails to teach control means for controlling the hash

value generation means and the public key encryption processing means, the control

means suppressing arithmetic operations performed by the public key encryption

processing means when the hash value generation means accesses the storage

means. However, in an analogous art Dyer teaches control means for controlling the

hash value generation means and the public key encryption processing means, the

control means suppressing arithmetic operations performed by the public key encryption

processing means when the hash value generation means accesses the storage means

(Dyer, Col. 5 Lines 14 – 20 and Col. 2 Lines 7 – 21).

At the time the invention was made, it would have been obvious to a person of

ordinary skill in the art to use Dyer's system for hash scanning of shared memory

interfaces with Garib's secret key messaging because it offers the advantage of being

faster to traverse the hash memory (Dyer, Col. 2 Lines 7 – 21).

7.   As per claims 2 and 14, Garib teaches the public key encryption processing

means includes a register group having a register for maintaining an arithmetic

operation value and a register for storing a result, the hash value generation means

includes a register group having a register for maintaining an arithmetic operation value

and a register for storing the generated hash value, at least the register group of the

public key encryption processing means and the register group of the hash value

generation means are shared (Garib, Col. 4 Lines 9 – 26 and Col. 12 Lines 16 – 19,

Garib teaches a comparison and the use of a processor, It is inherent that a processor

uses registers to perform tasks that involve comparing values) and the hardware is

switched in a time-shared manner depending upon the operation mode (Garib, Col. 12

Lines 16 – 19, It is inherent that a processor operates in a time shared manner).

8.   As per claims 5 and 17, Garib teaches the public key encryption processing

means includes public key encryption arithmetic operation core means for performing

various arithmetic operations for public key encryption (Garib, Col. 4 Lines 38 – 42,

IDEA is an arithmetic key generation means), the hash value generation means

includes hash value arithmetic operation core means for performing various arithmetic

operations for hash value generation (Garib, Col. 4 Lines 9 – 26, SHA-1 used for Hash

generation which is an arithmetic means for hash generation), and the public key

encryption arithmetic operation core means and the hash value arithmetic operation

core means are shared (Garib, Col. 4 Lines 62 – 67, Hash and key are used together).

9.   As per claims 6 and 18, Garib teaches the public key encryption arithmetic

operation core includes adder means, and shares the adder means with the hash value

arithmetic operation core means (Garib, Col. 4 Lines 9 – 26 and Col. 12 Lines 16 – 19,

Garib teaches a comparison and the use of a processor, It is inherent that a processor

uses adders to perform operations).

10.   As per claim 9, Garib teaches the hash value generation means stores the

generated hash value into the storage means at an address which is used by the public

key encryption processing means, and the public key encryption processing means

reads the hash value stored in the storage means (Garib, Col. 5 Lines 66 – 67 and Col.

6 Lines 1 – 6, generates a hash and stores the hash, addresses would be inherent).

11.   As per claim 11, Garib teaches the hash value generation means performs an

operation using the SHA-1 technique (Garib, Col. 4 Lines 9 – 26, SHA-1 used for Hash

generation).

12.   Claims 3, 4, 15 and 16 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Garib U.S. Patent No. (6,728,378) and Dyer et al. U.S Patent No.

(6,625,592) and in further view of Kaufman et al. U.S. Patent No. (5,764,772).

13.   As per claims 3 and 15, Garib teaches the common key encryption processing

means including a register group having a register for maintaining the resulting data and

a register for maintaining key data, wherein the register group of the common key

encryption processing means and the register group of the public key encryption

processing means are shared (Garib, Col. 4 Lines 9 – 26 and Col. 12 Lines 16 – 19,

Garib teaches a comparison and the use of a processor, It is inherent that a processor

uses registers to perform tasks that involve comparing values) but fails to teaches

common key encryption processing means for performing an encryption operation using

a common key encryption technique to generate a random number for use in the

encryption operation of the public key encryption processing means. However, in an

analogous art Kaufman teaches common key encryption processing means for

performing an encryption operation using a common key encryption technique to

generate a random number for use in the encryption operation of the public key

encryption processing means (Kaufman Col. 4 Lines 26 – 34).

At the time the invention was made, it would have been obvious to a person of

ordinary skill in the art to use Kaufman's differential work factor cryptography with

Garib's secret key messaging because it offers the advantage of creating a key based

on an unpredictable number which makes the key more secure (Kaufman Col. 4 Lines

26 – 34).

14.   As per claims 4 and 16, Garib as modified teaches the common key encryption

processing means performs the encryption operation using the DES technique

(Kaufman, Col. 1 Lines 38 – 44).

15.   Claims 7 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Garib U.S. Patent No. (6,728,378) and Dyer et al. U.S Patent No. (6,625,592) and in

further view of Kitamura U.S. PG-Publication No. (2002/0016917).

16.   As per claims 7 and 19, Garib fails to teach the public key encryption processing

means includes a bus switch for making the bit width variable, and the public key

encryption processing means shares the bus switch with the hash value generation

means. However, in an analogous art Kitamura teaches the public key encryption

processing means includes a bus switch for making the bit width variable, and the public

key encryption processing means shares the bus switch with the hash value generation

means (Kitamura, Paragraph 0085).

At the time the invention was made it, it would have been obvious to a person of ordinary skill in the art to use Kitamura's system integrated circuit with Garib's secret key messaging because it offers the advantage of high speed switching in a system.

17.   Claims 8 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Garib U.S. Patent No. (6,728,378), Dyer et al. U.S Patent No. (6,625,592) and Kitamura U.S. PG-Publication No. (2002/0016917), as applied to claim 7 and in further view of Kaufman et al. U.S. Patent No. (5,764,772).

18.   As per claims 8 and 20, Kitamura teaches, the common key encryption processing means including a bus switch, wherein the bus switch of the common key encryption processing means and the bus switch of the public key encryption processing means are shared (Kitamura, Paragraph 0085), but fails to teach further comprising common key encryption processing means for performing an encryption operation using a common key encryption technique to generate a random number for use in the encryption operation of the public key encryption processing means. However, in an analogous art Kaufman teaches further comprising common key encryption processing means for performing an encryption operation using a common key encryption technique to generate a random number for use in the encryption operation of the public key encryption processing means (Kaufman Col. 4 Lines 26 – 34).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Kaufman's differential work factor cryptography with

Garib's secret key messaging because it offers the advantage of creating a key based on an unpredictable number which makes the key more secure (Kaufman Col. 4 Lines 26 – 34).

19.   Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Garib U.S. Patent No. (6,728,378) and Dyer et al. U.S Patent No. (6,625,592) and in further view of Schneier, Applied Cryptography 2nd Edition.

20.   As per claim 10, Garib fails to teach the public key encryption processing means performs the encryption operation using the elliptic curve cryptosystem technique. However, in an analogous art Schneier teaches the public key encryption processing means performs the encryption operation using the elliptic curve cryptosystem technique (Schneier, Page 480, section 19.8).

At the time the invention was made, it would have been obvious to a person ordinary skill in the art to use Schneier's Applied Cryptography with Garib's secret key messaging because it offers the advantage of smaller key-sizes to create faster systems (Schneier, Page 480, section 19.8).

21.   Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Garib U.S. Patent No. (6,728,378) and Dyer et al. U.S Patent No. (6,625,592) and in further view of Inada U.S. Patent No. (6,986,044).

22.   As per claim 12, Garib fails to teach the encryption apparatus is incorporated in a non-contact IC card having a communication function. However, in an analogous art

Inada teaches the encryption apparatus is incorporated in a non-contact IC card having

a communication function (Inada, Col. 9 Lines 10 – 20).

At the time the invention was made it would have been obvious to a person of

ordinary skill in the art to use Inada's method for group unit encryption with Garib's

secret key messaging because it offers the advantage of having a secure storage for

encryption keys (Inada, Col. 9 Lines 10 – 20).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

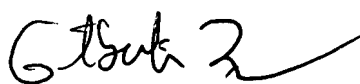than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Roderick Tolentino whose telephone number is (571) 272-2661. The examiner can normally be reached on Monday - Friday 9am to 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Roderick Tolentino
Examiner
Art Unit 2134

Roderick Tolentino

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100